AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

FILED

JAN 03 2019

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
INFORMATION ASSOCIATED WITH THE YAHOO! ACCOUNTS HONGJIN.TAN@YAHOO.COM AND LEWISTAN1983@YAHOO.COM, STORED AT PREMISES CONTROLLED BY OATH HOLDINGS INC. LOCATED AT 701 1ST AVENUE, SUNNYVALE, CA 92064

Case No. 19-mj-2-PJC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1832(a)	Theft of Trade Secrets
18 U.S.C. § 1030(a)(1)	Fraud and Related Activities in Connection with Computers

The application is based on these facts:

See Attached Affidavit by Brian S. Dean, SA, FBI

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of _____ days (give exact ending date if more than 30 days: 4/1/2019) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Brian S. Dean, SA, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/3/2019

Judge's signature

City and state: Tulsa, OK

US Magistrate Judge Paul J. Cleary
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE YAHOO! ACCOUNTS HONGJIN.TAN@YAHOO.COM AND LEWISTAN1983@YAHOO.COM, STORED AT PREMISES CONTROLLED BY OATH HOLDINGS INC. LOCATED AT 701 1ST AVENUE, SUNNYVALE, CA 92064.	Case No. 19-mj-2-PJC **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Brian S. Dean, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for information associated with certain Yahoo! Email accounts stored at premises controlled by Oath Holdings Inc. in Sunnyvale, California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo! to disclose to the government copies of the information (including the content of communications) further described in Attachments A and B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) assigned to the Oklahoma City Field Office, Tulsa Resident Agency. As a Special Agent, my duties include investigating violations of federal criminal law and threats to national security. In addition to formalized training, I have received extensive training through my involvement in numerous investigations working alongside experienced law enforcement officers at both the federal and local level. My investigations include, but are not limited to, counterterrorism, computer intrusions, drug and gang violations, and violent crimes.

3. The facts and circumstances of this investigation set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the circumstances described herein, and a review of public source information. This affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, and therefore does include each and every fact I have learned during the course of this investigation.

4. Based on my training, research, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of:

- Title 18, United States Code, Section 1832(a) – Theft of Trade Secrets;
- Title 18, United States Code, Section 1030(a)(1) – Fraud and Related Activities in Connection with Computers;

have been committed, and evidence of these crimes are located in the place described in Attachment A. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND CONCERNING EMAIL PROVIDER

5. Yahoo! was established in 1994, and provides a variety of on-line services including electronic mail ("email") to the public. Yahoo! allows subscribers to obtain email accounts at the domain name @yahoo.com to include the email accounts listed in Attachment A. Subscribers obtain an account by registering with Yahoo! and providing basic personal information. The servers maintained by Yahoo! are therefore likely to contain stored electronic communications and information concerning subscribers and their use of Yahoo! services, such as

account access information, email transaction information, and account application information. In my training and experience, such information may constitute as evidence of the crimes under investigation, and assist in corroborating the identity and intent of the account's user or users.

BACKGROUND CONCERNING COMPANY A

6. Company A was established in 1917, and is an international independent energy and petroleum corporation, focused on the exploration and development of petrochemical products and by-products, oil, and natural gas. Several years ago, Company A developed a cutting-edge Downstream Energy Market Product (hereafter referred to as Product A), and in the last year alone, has earned an estimated $1.4 to $1.8 billion from the sale and distribution of the product in interstate and foreign markets. Currently, there are only two refineries in the world capable of manufacturing Product A, and one is located in the Northern District of Oklahoma.

7. Company A's technological research, development, and processes associated with the production of Product A are critical to its business and are considered sensitive proprietary information. This information (hereinafter referred to as the Trade Secret Information), would be of significant value to Company A's competitors, and is therefore protected through a multi-layered strategy involving both physical security, as well as password protected computer systems.

8. Company A restricts access to the facility where Product A is produced. Magnetic card readers are utilized to gain access to the main building, and are again required to enter individual research divisions within. Only employees with an operational need-to-know are granted access to Trade Secret Information. Additionally, as a condition of their employment, all personnel are required to sign a non-disclosure agreement specifically prohibiting the distribution of any confidential and proprietary information, and or research products to other companies, persons, or countries.

9. Company A also has multiple data security policies in place stipulating all information created, sent, received, or stored on Company A's electronic resources is company property, and all activity on Company A's electronic resources is subject to monitoring. These policies prohibit employees from transmitting, receiving, or storing company information outside Company A's electronic resources.

BACKGROUND CONCERNING HONGJIN TAN

10. On 04/21/2017, Company A hired Hongjin Tan, a citizen of The People's Republic of China, as a research engineer in their battery development division in the Northern District of Oklahoma. According to the resume Tan provided Company A, Tan received a Bachelor of Science Degree in Physics from Nanjing University in Nanjing, China (2006), and a Master's Degree and Doctorate Degree from the California Institute of Technology in Pasadena, California (2011). While employed with Company A, Tan was responsible for the development of battery technology through the utilization of Company A proprietary information.

PROBABLE CAUSE

11. On 12/13/2018, at approximately 12:19 p.m. Eastern Time, Company A notified the FBI regarding possible theft of trade secrets at their primary facility in the Northern District of Oklahoma. According to a Company A representative, on 12/12/2018 at approximately 10:30 a.m., Tan provided his two weeks' notice to his supervisor, and said he was returning to China to take care of his aging parents. Tan said he did not currently have a job offer, but was negotiating with several battery companies in China. Tan's sudden and unforeseen resignation, coupled with the possibility of Tan seeking employment with a competitor, prompted Company A to revoke his access to company systems, and conduct a Systems Access review of his computer activity.

12. During the review, Company A security specialists noted Tan had recently accessed hundreds of files considered to be outside the scope of his employment. Among these files were multiple documents pertaining to the technical processes involved in the production of Product A, its use in cell-phone and lithium-based battery systems, as well as Company A's marketing strategy for Product A in China.

13. Security personnel escorted Tan to his supervisor's office where he was advised he would not be allowed to finish his final two weeks of employment, and was no longer authorized to be on Company A's property. Tan's personal bag and keys were searched, and then he was escorted off the premises. At approximately 4:00 p.m. that afternoon, Tan sent the following text message to his supervisor:

> ... [Another Company A supervisor] was asking if there is anything I have with me associated with company IP. I have a memory disk that contains lab data that I plan to write report on, and papers/reports I plan to read at home. Now that I have been exited from (COMPANY A), can you check what is the best way of handling the information and how sensitive they are? Can I still read the papers/reports from the memory disk?

After receiving the above text from Tan, Tan's supervisor asked him to return the flash drive to Company A. At approximately 5:15 p.m. on 12/12/18, Tan returned to the Research Technology Center at Company A, where he provided a personally owned USB flash drive to his supervisor. Tan's supervisor confirmed at no point was he issued a flash drive, nor was he authorized to utilize one over his company issued laptop to access work related information, especially information deemed to be outside his duties and responsibilities.

14. Using commercially available software, Company A security specialists reviewed the USB flash drive and discovered it contained data files (both deleted and undeleted) owned solely by Company A. Several of the documents were in fact marked "CONFIDENTIAL" or "RESTRICTED," and after further analyzation, it was determined these files in compilation with

one another, would provide a competing company the technical know-how to produce Product A. The unauthorized distribution of this information would have tremendous impact to Company A in terms of technological and economic loss.

15. These specific files were deleted from the flash drive on 12/12/2018, the day of Tan's resignation. This in direct violation of the Confidential Information, Non-Disclosure and Intellectual Property Agreement signed by Tan on 06/19/2018. Without prior written consent, employees are not to:

> "disclose, use, reproduce, or transmit (except for the performance of his duties for Company A), or permit the unauthorized disclosure, use, reproduction or transmission of any Confidential Information during the period of his employment with Company A or at any time thereafter...and upon leaving the employ of Company A, take any records, memoranda, drawings, pictures, models, papers, notebooks, reports, computer disks or other similar media having Confidential Information in or on such media."

16. Tan was reminded of this obligation every time he logged into his work computer by a warning banner which stated:

> This is a private computer system to be accessed and used for (Company A) business purposes. By accessing, using and continuing to use this system or device, you agree to the terms of use. All access must be specifically authorized and used only in accordance with all applicable (Company A) policies. Unauthorized access or use of this system is prohibited and may expose you to liability under criminal and civil laws. Absent a separate written agreement, all non-personal information and content you create, store or collect on behalf of (Company A) or in the scope of your employment, on this computer system is the sole property of (Company A). To the extent permitted under local law, (Company A) reserves the right to monitor, access, intercept, records, read, copy, capture and disclose all information received, sent through or stored in this system or device, without notice, for any purpose and at any time.

17. On 12/13/2018, one of Tan's co-workers filed a report with Company A security personnel. The co-worker said on 12/12/2018 while out to dinner with Tan, Tan told him he was leaving Oklahoma on 12/27/2018 to return to China. Tan said he had interviewed for a job with a Chinese company (hereafter referred to as Company B) during his last trip to China in September

2018, and had been in constant contact with the company since he was in graduate school at The California Institute of Technology.

18. According to their company website, Company B is an energy engineering company located in Xiamen, China, and has "developed two [battery] production lines so far, one for Li-ion battery cathode materials (such as lithium cobalt oxide, ternary cathode material, lithium manganese oxide, lithium iron phosphate, etc.) and the other for NiMH battery anode material (Hydrogen storage alloy)."

19. International travel records for Tan from United States (U.S.) Customs and Border Protection and U.S. Department of Homeland Security confirm Tan traveled from the Dallas/Ft. Worth, Texas International Airport to Peking, China on 9/15/2018. Tan returned to the Dallas/Ft. Worth, Texas International Airport via the Beijing, China Capital International Airport on 9/30/2018.

USE OF PERSONAL EMAIL

20. On 12/19/2018, Tan's laptop issued to him by Company A was forensically examined by technically trained FBI computer analysts. A scanned document bearing Company B's insignia was sent from Tan's work email to his personal Yahoo! account hongjin.tan@yahoo.com, and was located on the laptop. The letter was written in Chinese, dated 10/15/2018, and contained Tan's signature at the bottom with the date of 10/17/2018. An image of this letter was submitted to an FBI Chinese linguist who roughly translated the text of the letter as follows:

> This is a Position Hiring Agreement:
> Mister TAN Hongjin will be the Energy New Material Engineering Center Director [LT] in Xiamen. The letter includes his responsibilities in the management portion as well as his expertise area. TAN's annual salary will be 800,000 RMB. As soon as he starts, he will be compensated 400,000 RMB for introducing the talent. While you [TAN] are signing the contract, you must guarantee that the information you have already provided

> and will provide is real and effective; there is no false [information]. TAN must promise the confidentiality that he has not [released] to a third party company technology and operational related information. TAN must sign the agreement before 10/20/2018, and the agreement becomes valid [on] 1/1/2019.

21. Affiant interprets the letter to mean Tan has been offered a substantial position with Company B in Xiamen, China for a salary of 800,000 RMB (approximately $116,000 USD). Tan has provided Company B with information, or "talent" for which he will be compensated 400,000RMB (approximately $58,000 USD), and by signing the offer, he guaranteed the information was real, effective, and has not been provided to any other competing companies. Affiant also notes this offer was made approximately two weeks after Tan returned from China, and is in direct conflict with what he told his supervisor in his Exit Interview about not having a job lined up in China.

22. Tan took multiple steps to prepare for his departure from the United States. Documentation found on his personal thumb drive revealed Tan booked a flight to China with Xiamen Airlines on 11/1/2018 for a departure date of 12/27/2018. Tan provided a contact email of hongjin.tan@yahoo.com for this reservation. Tan also placed multiple furniture items, a TV, and his vehicle on Craigslist, with the first item (vehicle) being posted on 12/12/2018. On 12/19/2018, Tan visited multiple car dealerships in the Tulsa area in order to obtain an appraisal for said vehicle. The contact information he provided the Sales representative at Route 66 Chevy included an email address of lewistan1983@yahoo.com.

CONCLUSION

23. Based on the aforementioned facts and circumstances, Affiant believes there is probable cause to suggest information maintained by Yahoo! on Hongjin Tan's email accounts hongjin.tan@yahoo.com and lewistan1983@yahoo.com contain evidence, fruits, and or instrumentalities of violations of statutes as previously noted. I therefore respectfully request this

Court to issue a search warrant for the location listed in Attachment A and the items listed in Attachment B.

24. Due to the fact Yahoo!, upon receipt of this warrant, will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time, day or night. Additionally, pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

25. Affiant further requests the Court order all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents as premature disclosure may give targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, and or notify confederates.

Respectfully Submitted,

Brian S. Dean
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 3rd day of January 2019.

Honorable Paul J. Cleary
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A – PROPERTY TO BE SEARCHED

This warrant applies to information associated with Yahoo! email accounts:

- hongjin.tan@yahoo.com
- lewistan1983@yahoo.com

For a time period of 01/01/2017 through present

stored at premises owned, maintained, controlled, or operated by Yahoo!, a company headquartered at 701 1st Avenue, Sunnyvale, California 92064.

ATTACHMENT B – ITEMS TO BE SEIZED

I. Information to be disclosed by Yahoo!

To the extent the information described in Attachment A is within the possession, custody, or control of Yahoo!, including any messages, records, files, logs, or information that have been deleted but are still available to Yahoo!, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Yahoo! is required to disclose the following information to the government:

a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

b. All past and current usernames, account passwords, and names associated with the accounts;

c. The dates and times at which the accounts and profiles were created, and the Internet Protocol ("IP") address at the time of sign-up;

d. All IP logs and other documents showing the IP address, date, and time of each login to the accounts;

e. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

f. All emails sent, received, "favorited," or forwarded by the account, and all photographs, images, or attachments included in those emails;

g. All location data associated with the accounts;

h. All data and information deleted by the users;

i. All privacy and account settings;

j. Accounts linked to the target accounts by cookies.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of:

- Title 18, United States Code, Section 1832(a) – Theft of Trade Secrets;
- Title 18, United States Code, Section 1030(a)(1) – Fraud and Related Activities in Connection with Computers.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Yahoo!, and my official title is _____. I am a custodian of records for Yahoo!. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Yahoo!, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Yahoo!; and

c. such records were made by Yahoo! as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date:_____ Signature:_____